REMARKS

Claims 1-40 are pending in the present application. Claims 37, 38, and 20 have been canceled. Independent Claims 1, 3, 26, 36, and 40 are currently amended. The amendment of the independent Claims 1, 3, 26, 36 and 40 is fully supported by the specification on page 4 lines 1-23 and Claim 20. Furthermore, Claim 36 incorporates the limitations of Claims 37 and 38 and, further, the element of an NMS, which generates a request that selectively retrieves network access data. Dependent Claims 37 and 38 are canceled. Dependent Claims 12, 18, 21, and 22, depending on Claim 1 or an intervening claim, have been amended to delete duplicitous language in the preamble, or in introductory phrases, or to correct dependency on a canceled claim. Dependent Claim 39 is amended to accommodate the cancellation of Claim 37 from which it depended.

Claims 1-3, 5, 9-10, 20, and 40 stand rejected under 35 U.S.C. 102(e) as being anticipated by North et al. [U.S. Pat. No. 6,505,245]. As to Claims 1-3 and 40, North teaches the invention as claimed includes a method of managing a telecommunications network, comprising: storing user profile data corresponding to a user profile in a first data repository [16, Fig. 1 or 28, 30, Fig. 2; 116, Fig. 5; col. 5, lines 28-40; i.e., the first data repository is a central data repository]; storing network device data corresponding to a network device in the telecommunications network in a second data repository [col. 7, lines 58-62; i.e., the network device data are originally stored locally (embedded) with each device]; detecting a request from a user for network device data corresponding to the network device, wherein the user request is associated with the user profile; generating a data access request to the second data repository utilizing the user profile data from the first data repository; and retrieving network device data from the second data repository in accordance with the user request. [For the last three limitations, see e.g., col. 4, line 42 - col. 5, line 60; col. 5, lines 3-11; col. 10, line 37 - col. 11, line 9; and col. 16, line 38 - col. 17, line 9].

Applicants' Claims 1, 3, and 40 (as currently amended) are not taught by North. In Fig. 2, North teaches that the consoles 38, 36 and 32 interface the manageable devices 26-1 through 26-N via computers 54, 52 and 50 through management terminal 30. In contrast Applicants' Fig 2 teaches that a console interface 852 utilizes a NMS program, having a client 850 and a server

851. North does not teach the claimed NMS client and server, which generates requests that selectively retrieve network access data from the second data repository utilizing the user profile data from the first data repository. Furthermore, North doesn't teach what data is stored nor where the data is stored. Additionally, North does not teach the use of two repositories.

Examiner states, as to Claim 5, North further teaches displaying the retrieved network device data in a user interface [col. 8, lines 23-33]. Applicants disagree. North states in col. 8, lines 23-33, "As previously set forth, it is contemplated that the system administrator of the management terminal 30 may manage the computing devices 26-1 through 26-N from a selected one of the consoles 28, 32, 36, or 38. It is contemplated that, in addition to a video monitor for *displaying information transmitted thereto by the management terminal 30*, each of the consoles 28, 32, 36, and 38 further include a conventionally configured keyboard, mouse or other data input device for generating instructions for the computing devices 26-1 through 26-N for transfer to the management terminal 30." North is **not** teaching the use of an interface to view the network device data (i.e. the data in the repositories).

Examiner states, as to Claims 9-10, North further teaches that the user profile data includes a group access level [col. 5, lines 22-27; col. 14, lines 39-44], wherein authorized users of the group must have a corresponding password [col. 5, lines 3-4].

Applicants' Claims 9-10 are dependent claims depending from Claims 1 and 9, respectively, and because dependent claims have all the limitations of the parent claims and, as such, should be allowed.

As to Claim 20, Examiner states that North further teaches detecting a request from a user for network device data, comprises: detecting the user request through a network management system (NMS) client [e.g., 50-54, Fig. 2]; and sending the user request from the NMS client to an NMS server [28, 30, Fig. 2], wherein the NMS server generates the data access request to the second data repository utilizing the user profile data from the first data repository and retrieves network device data from the second data repository in accordance with the user

request [col. 2, line 66 - col. 3, line 10]; and wherein the method further comprises: sending the retrieved network device data from the NMS server to the NMS client [col. 7, lines 17-29].

Claim 20 is canceled.

The amendments to the claims overcome the rejections of Claims 1-3, 5, 9-10, 20, and 40 as rejected under 35 U.S.C. 102(e). North does not teach the elements of a *network management system client*, a *network management system server*, wherein a request from a user through the network management system client for network device data corresponding to the network device, wherein the user request is associated with the user profile, and generating a data access request by the network management system server to s*electively retrieve network access data* from the second data repository utilizing the user profile data from the first data repository; and *retrieving network device data from the second data repository* in accordance with the user request. Substantially, North teaches hardware comprising multiple computer systems filtered through a management terminal in connection with manageable devices. In contrast, Applicants teach and claim software comprising a logical system for processing and storing data for managing a telecommunications network.

Claims 4, 6-8 and 12-16 stand rejected under 35 U.S.C. 103(a) as being unpatentable over North et al. (hereafter "North") [U.S. Pat. No. 6,505,245], as applied to claims 1-3, 5, 9-10, and 20 above.

As to Claim 4, North teaches that the profile data, together with other data spaces, are part of an organized memory subsystem [see Fig. 5]. North does not specifically teach that the first and second data can be stored in databases. However, for ease of data query and maintenance storing a plurality of mutually relevant data items in a database (e.g., in the form of relational database) is well known in the art. It would have been obvious to one of ordinary skill in the art at the time the invention was made that North's first and second data can be stored in databases because North's first and second data are subject to frequent accesses, and by organizing North's first and second data repository as databases would facilitate the data retrieval and maintenance.

Applicants agree that relational databases are well known. What is novel is isolating databases repositories as to client requests and generation of server requests.

As to Claims 6 and 8, Examiner admits that North does not specifically teach that the user profile data includes an IP address assigned to the network device. However, Examiner asserts that North teaches in one scenario that a remote console may manage a plurality of devices via the Internet [Fig. 1b; col. 1, line 67-col. 2, line 16] and in another scenario that a plurality of remote consoles may manage a plurality of devices by connecting the remote consoles to a central managing terminal via the Internet [Fig. 2]. As such, it is obvious that North's system/method applies to a combined scenario wherein the central managing terminal is only a node in the entire Internet, and communicating from each individual managing console to a managed device would require an IP address that is pre-assigned to the device.

Under such circumstances, it is obvious to one of ordinary skill in the art that the pre-assigned IP address can be included in each of the user profiles because each of North's remote console has to retrieve information associated with the user's pre-assigned role including which devices can be managed by the remote console and it would facilitate the database management by associating the IP addresses that are assigned to each individual console in the user profile.

Note that, in a sense, the central terminal of North's system functions as a domain name server for the remote managing consoles because the IP addresses of the managed devices are determined at the central terminal.

Patent Examiners carry the responsibility of making sure that the standard of patentability enunciated by the Supreme Court and by the Congress is applied in each and every case. The Supreme Court in *Graham v. John Deere*, 383 U.S. 1, 148 USPQ 459 (1966).

Under Section 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Office policy has consistently been to follow *Graham*

v. John Deere Co. in the consideration and determination of obviousness under 35 U.S.C. 103. The four factual inquires for determining obviousness is briefly as follows:

(A) The claimed invention must be considered as a whole;

(B) The references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination;

(C) The references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention; and

(D) Reasonable expectation of success is the standard with which obviousness is determined.

Applicants assert that the Examiner has not met the hindsight criteria (C) for obviousness. The central computer that Examiner is referencing in North, we suppose is. 34, which is identified as the Internet in Fig. 2. Taken to the Examiner's logical conclusion, one would surmise that the Internet connection taught by North teaches a user profile data that includes an IP address assigned to the network device; a user profile data that further includes a port identification for a port on the network device, and a user profile data that includes a Domain Name. Typically, these Internet connections are often dynamic and can take multiple routes, independent of a user profile. Also, North teaches a connection directly to the management terminal, as indicated by the dashed line. Furthermore, Applicants had no access to North, which was filed on August 22, 2000 claiming a priority filing date of April 13, 2000. Applicants filed on November 1, 2000. Applicants could not view the reference, and had no benefit of hindsight vision, as does the Examiner. North does not meet criteria (C) for a 103 rejection.

As to Claim 7, North further teaches that the user profile data further includes a port identification for a port on the network device [col. 4, lines 41-45 and 61-65; 30, 41-1 – 41 - N, Fig. 2].

Applicants' Claim 7 is a dependent claim, depending on intervening Claim 6 and parent Claim 1, and as such has all the limitations of both claims. These limitations have been previously discussed. Examiner has failed to meet the obviousness criteria C for Claims 6 and 8, and by its dependency on Claim 6, the criteria for Claims 7. Therefore, Claims 6-8 should be allowed.

As to Claims 12-16, the Examiner states that North teaches substantially the invention as presented in the claims above. North further teaches that devices are arranged in logical groups with events of each group associated with a respective console, which may in turn be referenced by the group name when defining action for an event [See Abstract and col. 5, lines 22-27]. Thus, although North does not specifically teach how the group name is being used in identifying and retrieving device data from the second data repository, it is noted that such features are rather obvious to a person of ordinary skill in the art because the group name is now part of the key indices in North's database and the use of it would facilitate retrieval of authorized user information and device data from the related database.

Applicants have accented that relational databases are well known. What is novel is isolating databases repositories as to client requests and generation of server requests. Dependent Claims 12-16 should be allowed.

Claims 11 and 17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over North et al. (hereafter "North") [U.S. Pat. No. 6505245], as applied to Claims 1-10, 12-16 and 20 above, further in view of Lim [U.S. Pat. No. 6,434,619]. As to Claim 11, the system communicates to managed devices via SNMP protocol [col. 3, lines 7-10]. North does not specifically teach that the user profile data includes a simple network management protocol (SNMP) community string. However, in the same field of endeavor, Lim teaches an Internet-based service management system wherein SNMP command string and user attributes are stored in a repository (e.g., a user profile included in a relational database) for allowing a remote operator to configure network elements in accordance with specific requirements [col. 3, lines 1-29; col. 17, lines 35-38].

In light of Lim's teaching, it would have been obvious to one of ordinary skill in the art to have included the SNMP community string in North's user profile data because the SNMP community string is specific in accordance with the level of access right assigned to each user and by including the SNMP community string it would facilitate the access of such information from the database. As to Claim 17, North teaches that the first and second data repositories are part of memory subsystems. North does not specifically teach that the data repositories are relational databases and the user profile data is stored in at least one table within the first database and network device data is stored in at least one table within the second database. However, Lim teaches that the repositories can be in the form of relational databases [e.g., col. 3, lines 10-29], wherein storing the user profile data and network device data in a respective table within each database is an obvious option. In light of Lim's teaching, it would have been obvious to one of ordinary skill in the art to also organize North's repositories as relational databases because it would facilitate the query from a remote operator for information stored therein.

Applicants have amended claim 1 to include that there is a network management system client for network device data corresponding to the network device, wherein the user request is associated with the user profile; and generating a data access request by the network management system server to selectively retrieve network access data from the second data repository utilizing the user profile data from the first data repository. Neither Lim nor North teaches this method. The rejections to Claims 11 and 17 are respectfully traversed.

Claims 18-19 and 21-39 stand rejected under 35 U.S.C. 103(a) as being unpatentable over North et al. (hereafter "North")[U.S. Pat. No. 6505245], as applied to Claims 1-17 and 20 above, further in view of Official Notice. s to Claims 18-19, North does not specifically teach generating, after detecting a user's logon request, a user profile logical managed object (LMO) including at least a portion of the user profile data from the first data repository and use the LMO to request access to the second data repository utilizing the user profile data from the LMO. However, Official Notice is taken that logical managed object for repeated access to a designated device or web server such as a cookie is well known in the art.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate a LMO similar to a cookie after a user's logon request is detected because by applying the LMO in the authentication and authorization process, it could prevent a user from repeating the logon process whenever a new connection session to the same target device or website is intended. As to Claims 21-26, since the features of these claims can also be found in claims 1,18 and 20, they are rejected for the same reasons set forth in the rejection of claims 1,18 and 20 above. As to Claim 31, North further teaches that the network device data retrieved from the second data repository comprises configured resource data associated with the group name [col. 4, line 61- col. 5, line 2. As to Claims 27-30 and 32-39, since the features of these claims can also be found in claims 1-4, 12, 14-16,18, 26 and 36-37, they are rejected for the same reasons set forth in the rejection of claims 1-4, 12, 14-16,18, 26 and 36-37 above.

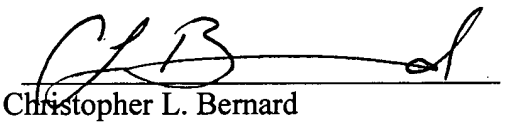
Applicants have amended Claim 18 to read on a user profile LMO to generate the data access request. Neither North nor Examiner's Official Notice teaches this limitation. Claim 19 depends on Claim 18, and is allowed by virtue of its dependency. Claims 21-25 depend on Claim 1, and the arguments for Claim 1 are applicable. Claims 37-39 are canceled. Independent Claim 26 has been amended to include the limitation of a network management system client for network device data corresponding to the network device, wherein the user request is associated with the user profile; and generating a data access request by the network management system server to selectively retrieve network access data from the second data repository utilizing the user profile data from the first data repository. The limitation is not taught by North or the Examiner's Official Notice, and the claims should now be allowable. Dependent Claims 27-35 depending on Claim 26 should now be allowed for the reasons cited above.

CONCLUSION

Applicants would like to thank Examiner for the attention and consideration accorded the present Application. Should Examiner determine that any further action is necessary to place the Application in condition for allowance, Examiner is encouraged to contact undersigned Counsel at the telephone number, facsimile number, address, or email address provided below. It is not believed that any fees for additional claims, extensions of time, or the like are required beyond those that may otherwise be indicated in the documents accompanying this paper. However, if such additional fees are required, Examiner is encouraged to notify undersigned Counsel at Examiner's earliest convenience.

Respectfully submitted,

Date: October 6, 2005



Christopher L. Bernard
Attorney for Applicants
Registration No.: 48,234

F. Rhett Brockington, Ph.D
Agent for Applicants
Registration No.: 29,618

DOUGHERTY, CLEMENTS, HOFER, BERNARD & WALKER
1901 Roxborough Road, Suite 300
Charlotte, North Carolina 28211 USA
Telephone: 704.366.6642
Facsimile: 704.366.9744
cbernard@worldpatents.com